IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Brian YEN	Examiner:	Jalatee WORJLOH
Serial No.:	09/900,803	Art Unit:	3621
Filed:	July 6, 2001		
Title:	SYSTEM AND METHOD FOR ON-DEMAND DATA DISTRIBUTION IN A P2P SYSTEM		

Mail Stop Appeal Briefs - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF OF BRIAN YEN IN U.S. PATENT APPLICATION NO. 09/900,803

(1) Real Party in Interest:

The real party in interest is the applicant/inventor, Brian Yen.

(2) Related Appeals and Interferences:

There are no related appeals or interferences known to the appellant or the appellant's legal representative that will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims:

Claims 1 – 42 and 44 – 81 are pending and stand rejected in the above-identified patent application. Claim 43 is cancelled. Claims 1 – 42, and 44 – 81 are on appeal. The claims on appeal are listed in an attached appendix.

(4) Status of Amendments:

There has been no amendment filed subsequent to final rejection.

(5) Summary of Claimed Subject Matter:

The present invention provides a system for distributing data via a P2P network topography. The system comprises a server 110 communicatively coupled to a network, such as the Internet 120. A plurality of consumer boxes 130, 140, 150, which may include mobile devices, computers, or any other network-enabled device (which may also be generically referred to as peers), may also be coupled to the network 120. The central server 110 includes a distribution engine 350, which keeps a database 360 of files available over the network at consumer boxes 130, 140, 150, as well as consumer boxes' addresses 530. A database 370 keeps consumer box owner data, which may include name, address, and payment information, as well as other data. Upon receiving a request for a data file in storage 520 or 550 from a consumer box 130, 140, or 150, the distribution engine 350 locates a consumer box 130, 140, or 150 closest to the requesting consumer box that has the requested data file. The distribution engine 350 then sends information to the requesting consumer box necessary to download the data file from the closest consumer box storage 520 or 550. This information may include the address of the closest consumer box, encryption data to decrypt the request data file, and other data. The distribution engine may also request payment information from the requesting consumer box and process payment.

The present invention further provides a method for P2P data distribution. The method comprises receiving 615 a request from a consumer box for a data file, the request including payment information; locating 655 a consumer box closest to the requesting consumer box having the requested file; sending 660 encryption data to decrypt the request data file to the requesting consumer box; sending the address 660 of the closest consumer box to the requesting consumer box; and processing 650 payment for the requested file.

Therefore, the system and method advantageously prevent theft of intellectual property in P2P systems by enabling encryption and payment for authorized duplication of intellectual property. (From the Summary on page 3 – 4 of the Application as filed).

Claims 31 and 81 are means plus function claims as permitted by 35 USC 112, sixth paragraph. The claimed means plus function and corresponding structure are identified below:

31. means for receiving , from a first peer, a request for a data file, the request including an ID of the first peer; **[distribution engine 350; first full paragraph of Page 11]**

means for identifying a second peer having the data file from an index of peers; **[distribution engine 350; last paragraph of Page 13]**

means for processing payment for the data file based on the ID of the first peer **[distribution engine 350; first full paragraph of Page 13]**; and

means for sending, to the first peer, an address of the second peer and decryption information to decrypt the data file. **[distribution engine 350; first paragraph of Page 11]**

81. means for sending, to a server, a purchase request for a data file, the purchase request including a peer identifier; **[consumer engine 510; second paragraph of Page 14]**

means for receiving, from the server, an address of a second peer having the data file and a first encryption dataset for decrypting the data file; **[consumer engine 510; second paragraph of Page 14]**

means for sending, to the second peer, a download request for the data file; **[consumer engine 510; last paragraph of Page 15]**

means for receiving, from the second peer, the data file; **[consumer engine 510; last paragraph of Page 15]**

means for decrypting the data file with the first encryption dataset; **[consumer engine 510; first paragraph of Page 16]**and

means for outputting the data file. **[Audio Output 420; last paragraph on Page 8]**

(6) Grounds of Rejection to be Reviewed on Appeal:

(I) Whether claims 1 and 16 are unpatentable under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter.

(II) Whether claims 1 – 4, 8, 10 – 19, 23, 25 – 35, 39 – 49, 51, 53 – 60, 62, 64 – 71, 73, 75 – 81 are unpatentable under 35 U.S.C. §103(a) over "How the Old Napster Worked" by Jeff Tyson (hereinafter *Tyson*) in view of U.S. Publication No. 2001/0051996 to Cooper et al. (hereinafter *Cooper*).

(III) Whether claims 5 – 7, 9, 20 – 22, 24, 36, 50, 52, 61, 63, 72 and 74 are unpatentable under 35 U.S.C. §103(a) over *Tyson* in view of *Cooper* and further in view of U.S. Publication No. 2001/0051996 to Hunter et al. (hereinafter *Hunter*).

(7) Arguments:

(I) The Examiner rejected claims 1 and 16 under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter. The Examiner states that the claims are directed to a process that does nothing more than manipulate an abstract idea. Applicant submits that claims 1 and 16 are patentable under 35 U.S.C. § 101.

Applicant respectfully submits that claims 1 and 16 are directed to the technological arts by reciting components such as servers and peers. A server by plain meaning and as defined in the Merriam Webster Online Dictionary is "a computer in a

network that is used to provide services (as access to files or shared peripherals or the routing of e-mail) to other computers in the network." http://www.m-w.com/cgi-bin/dictionary?book=Dictionary&va=server. A peer by plain meaning and as defined in Wikipedia is a "peer-to-peer computer networking participant, acting as both client and server." http://en.wikipedia.org/wiki/Peer.

Further, the claims do more than manipulate abstract ideas. Specifically, the claims recite the transmission of data and the identification of where the data is located. With the transmitted data, a peer can then obtain and decrypt data, such as a song. Further, the data is transmitted upon payment, thereby providing a data rights management system based on payment for data, thereby preventing unauthorized transmission of data. Accordingly, the claims are directed to a method that produces a concrete result (transmission of location and decryption data), tangible result (the data is then stored at a new location) and a useful result (digital rights management).

(II) Applicant submits that claim 1 is patentable under 35 U.S.C. §103(a) over *Tyson* and *Cooper* by at least reciting:

> A method for implementation in an index server in a peer-to-peer system, comprising:
> receiving, from a first peer, a request for a data file, the request including an ID of the first peer;
> identifying a second peer having the data file from an index of peers;
> processing payment for the data file; and
> sending, to the first peer, an address of the second peer and a first encryption dataset to decrypt the data file.

As the Examiner states in the Office Action, neither *Tyson* nor *Cooper* teach all of the steps claimed. However, the Examiner combines the references to yield the claimed invention stating that one of ordinary skill in the art would have

been motivated to do this because it prevents unauthorized individuals from accessing the digital content thus reducing piracy.

Applicant respectfully submits that it would not have been obvious to combine the references as no one has done so since the failure of Napster due to a lack of a digital rights management component. Even today, there is no Peer to Peer (P2P) system that solves the digital rights management issue and therefore prevents piracy. In fact, Napster ceased their P2P file sharing system because of copyright violations and the inability to combine a P2P system with a digital rights management system. The current version of Napster no longer enables the transfer of files between peers. Accordingly, Napster's P2P system was in effect a failed experiment and is therefore unavailable as prior art as the Federal Circuit held in *Fromson v. Advance Offset Plate, Inc.*, 225 USPQ 26, 33:

> The "failed" experiment reported in the prosecution history of the Mason patent renders that patent irrelevant as a prior art reference. As stated by Judge Learned Hand, "another's experiment, imperfect and never perfected will not serve either as an anticipation or as part of the prior art, for it has not served to enrich it." *Picard v. United Aircraft Corp.*, 128 F.2d 632, 635, 53 USPQ 563, 566 (2d Cir. 1942), *cert. denied*, 317 U.S. 651 (1942).

Further, the history of Napster teaches away from incorporating a digital rights management system because of the failure of Napster to do so and to instead reinvent itself as a conventional file downloading service. Since the history teaches away from the claimed invention, there would be no motivation to combine the cited references. Further, there is no suggestion to combine or modify Napster in the cited references. *Tyson* concludes that "P2P is here to stay, regardless of legality disputes," thereby suggesting there is no solution to the legal

issue of digital rights managements. As the Federal Circuit held in *In re Gurley*, it is not obvious to combine the references because the line of development in *Tyson* teaches away from digital rights managements as Napster converted to a conventional file downloading service and other P2P systems that came afterwards have not solved this problem.

> A reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant. The degree of teaching away will of course depend on the particular facts; in general, a reference will teach away if it suggests that the line of development flowing from the reference's disclosure is unlikely to be productive of the result sought by the applicant. *See United States v. Adams*, 383 U.S. 39, 52, 148 USPQ 479, 484 (1966) ("known disadvantages in old devices which would naturally discourage the search for new inventions may be taken into account in determining obviousness"). *In re Gurley*, 31 USPQ2d 1130, 1131 (Fed Cir. 1994).

As the rejections of the other claims also rely on *Tyson*, they are patentable over the cited references for the same reasons.

Further, claims 2, 3, 17, 18, 33, and 34 were rejected by the Examiner even though *Tyson* and the other references do not teach the elements of these claims. The claims are not non-functionally descriptive as they recite positive actions. The Examiner cites no art that anticipates these claims.

(III) Claims 5 – 7, 9, 20 – 22, 24, 36, 50, 52, 61, 63, 72 and 74 are patentable under 35 U.S.C. §103(a) over *Tyson* in view of *Cooper* and further in view of *Hunter* for the reasons cited above with respect to *Tyson*. Since *Tyson* is unavailable per the above, the combination of references does not teach the claimed invention.

(8) Appendix: Claim Listing

1. (Original) A method for implementation in an index server in a peer-to-peer system, comprising:

receiving, from a first peer, a request for a data file, the request including an ID of the first peer;

identifying a second peer having the data file from an index of peers;

processing payment for the data file; and

sending, to the first peer, an address of the second peer and a first encryption dataset to decrypt the data file.

2. (Previously Presented) The method of claim 1, wherein the identifying comprises identifying a second peer geographically closest to the first peer.

3. (Previously Presented) The method of claim 1, wherein the identifying comprises identifying a second peer having a lowest number of pings in relation to the first peer.

4. (Original) The method of claim 1, wherein the data file is a music file.

5. (Original) The method of claim 1, further comprising:

selecting an advertisement to send to the first peer; and

sending, to the first peer, an address of a peer having the advertisement.

6. (Original) The method of claim 5, wherein the selecting an advertisement is based on demographic data associated with the first peer.

7. (Original) The method of claim 5, wherein the processing payment processes a reduced payment for the data file upon sending, to the first peer, the address of a peer having the advertisement.

8. (Original) The method of claim 1, further comprising verifying a password from the first peer before processing payment and sending, to the first peer, the address of the second peer.

9. (Original) The method of claim 1, wherein the processing does not occur until receipt, from the first peer, of a confirmation signal confirming receipt of the data file.

10. (Original) The method of claim 1, further comprising:

upon receipt, from the first peer, of a signal indicating inability to retrieve the data file

identifying another peer having the data file from an index of peers;

sending, to the first peer, an address of the another peer and another encryption dataset to decrypt the data file.

11. (Original) The method of claim 1, further comprising updating the index of peers to indicate that the first peer includes a copy of the data file.

12. (Original) The method of claim 1, further comprising sending a second encryption dataset to the second peer.

13. (Original) The method of claim 12, wherein the second encryption dataset includes an encrypted public transaction key and an encrypted public key, the public key capable to encrypt data so that the encrypted data is decipherable only by the first peer.

14. (Original) The method of claim 1, wherein the first encryption dataset includes an encrypted private transaction key.

15. (Original) The method of claim 14, wherein the encrypted private transaction key is decipherable only by the first peer.

16. (Previously Presented) A machine-readable medium, for use in an index server in a peer-to-peer system, the medium having stored thereon instructions to:

receive, from a first peer, a request for a data file, the request including an ID of the first peer;

identify a second peer having the data file from an index of peers;

process payment for the data file based on the ID of the first peer; and

send, to the first peer, an address of the second peer and a first encryption dataset to decrypt the data file.

17. (Previously Presented) The machine-readable medium of claim 16, wherein the instruction to identifying comprises identifying a second peer geographically closest to the first peer.

18. (Previously Presented) The machine-readable medium of claim 16, wherein the instruction to identify comprises identifying a second peer having a lowest number of pings in relation to the first peer.

19. (Original) The machine-readable medium of claim 16, wherein the data file is a music file.

20. (Original) The machine-readable medium of claim 16, further comprising instructions to:

select an advertisement to send to the first peer; and

send, to the first peer, an address of a peer having the advertisement.

21. (Original) The machine-readable medium of claim 20, wherein the instruction to select an advertisement is based on demographic data associated with the first peer.

22. (Original) The machine-readable medium of claim 20, wherein the instruction to process payment processes a reduced payment for the data file upon sending, to the first peer, the address of a peer having the advertisement.

23. (Original) The machine-readable medium of claim 16, further comprising an instruction to verify a password from the first peer before processing payment and sending, to the first peer, the address of the second peer.

24. (Original) The machine-readable medium of claim 16, wherein the instruction to process does not occur until receipt, from the first peer, of a confirmation signal confirming receipt of the data file.

25. (Original) The machine-readable medium of claim 16, further comprising instructions to,

upon receipt, from the first peer, of a signal indicating inability to retrieve the data file,

identify another peer having the data file from the index of peers;

send, to the first peer, an address of the another peer and another encryption dataset to decrypt the data file.

26. (Original) The machine-readable medium of claim 16, further comprising an instruction to update the index of peers to indicate that the first peer includes a copy of the data file.

27. (Original) The machine-readable medium of claim 16, further comprising an instruction to send a second encryption dataset to the second peer.

28. (Original) The machine-readable medium of claim 27, wherein the second encryption dataset includes an encrypted public transaction key and an encrypted public key, the public key capable to encrypt data so that the encrypted data is decipherable only by the first peer.

29. (Original) The machine-readable medium of claim 16, wherein the first encryption dataset includes an encrypted private transaction key.

30. (Original) The machine-readable medium of claim 29, wherein the encrypted private transaction key is decipherable only by the first peer.

31. (Original) An index server for use in a peer-to-peer system, comprising:

means for receiving, from a first peer, a request for a data file, the request including an ID of the first peer;

means for identifying a second peer having the data file from an index of peers;

means for processing payment for the data file based on the ID of the first peer; and

means for sending, to the first peer, an address of the second peer and decryption information to decrypt the data file.

32. (Original) An index server for use in a peer-to-peer system, comprising:

a data file index capable to store listings of data files, peers storing the data files, and encryption data needed to decrypt the data files;

a distribution engine, communicatively coupled to the index, capable to

receive, from a first peer, a request for a data file, the request including an ID of the first peer;

identify a second peer having the data file from the index;

process payment for the data file based on the ID of the first peer; and

send, to the first peer, an address of the second peer and a first encryption dataset to decrypt the data file.

33. (Previously Presented) The server of claim 32, wherein the distribution engine identifies a second peer that is geographically closest to the first peer.

34. (Previously Presented) The server of claim 32, wherein distribution engine identifies a second peer having a lowest number of pings in relation to the first peer.

35. (Original) The server of claim 32, wherein the data file is a music file.

36. (Original) The server of claim 32, wherein the distribution engine is further capable to:

select an advertisement to send to the first peer; and

send, to the first peer, an address of a peer having the advertisement.

37. (Original) The server of claim 36, wherein the distribution engine is further capable to select an advertisement based on demographic data associated with the first peer.

38. (Original) The server of claim 36, wherein the distribution engine is further capable to process a reduced payment for the data file upon sending, to the first peer, the address of a peer having the advertisement.

39. (Original) The server of claim 32, wherein the distribution engine is further capable to verify a password from the first peer before processing payment and sending, to the first peer, the address of the second peer.

40. (Original) The server of claim 32, wherein the distribution engine is further capable to delay processing until receipt, from the first peer, of a confirmation signal confirming receipt of the data file.

41. (Original) The server of claim 32, wherein the distribution engine is further capable to,

upon receipt, from the first peer, of a signal indicating inability to retrieve the data file,

identify another peer having the data file from the index; and

send, to the first peer, an address of the another peer and another encryption dataset to decrypt the data file.

42. (Original) The server of claim 32, wherein the distribution engine is further capable to update the index to indicate that the first peer includes a copy of the data file.

43. (Canceled).

44. (Original) The server of claim 32, wherein the distribution engine is further capable to send a second encryption dataset to the second peer.

45. (Original) The server of claim 44, wherein the second encryption dataset includes an encrypted public transaction key and an encrypted public key, the public key capable to encrypt data so that the encrypted data is decipherable only by the first peer.

46. (Original) The server of claim 32, wherein the first encryption dataset includes an encrypted private transaction key.

47. (Original) The server of claim 36, wherein the encrypted private transaction key is decipherable only by the first peer.

48. (Original) A method for implementation in a first peer in a peer-to-peer system, comprising:

sending, to a server, a purchase request for a data file, the purchase request including a peer identifier;

receiving, from the server, an address of a second peer having the data file and a first encryption dataset for decrypting the data file;

sending, to the second peer, a download request for the data file;

receiving, from the second peer, the data file;

decrypting the data file with the first encryption dataset; and

outputting the data file.

49. (Original) The method of claim 48, wherein the data file is a music file.

50. (Original) The method of claim 48, further comprising:

receiving, from the server, an address of a peer having an advertisement;

downloading, from the peer having the advertisement, the advertisement; and

playing the advertisement.

51. (Original) The method of claim 48, further comprising sending a password to the server before receiving the address of a second peer having the data file and the first encryption dataset for decrypting the data file.

52. (Original) The method of claim 48, further comprising sending, to the server, a confirmation signal confirming receipt of the data file.

53. (Original) The method of claim 48, further comprising sending, to the server, a signal indicating inability to download the data file when unable to download the data file.

54. (Original) The method of claim 53, further comprising receiving an address of a third peer having the data file after sending the signal indicating inability to download the data file.

55. (Original) The method of claim 48, wherein the first encryption dataset includes an encrypted private transaction key.

56. (Original) The method of claim 55, wherein the encrypted private transaction key is decipherable only by the first peer.

57. (Original) The method of claim 55, decrypting the data file using the private transaction key and a private key only known to the first peer.

58. (Original) The method of claim 48, further comprising:

storing an encrypted copy of the data file; and

notifying the server that the data file is stored.

59. (Previously Presented) A machine-readable medium, for use in a peer in a peer-to-peer system, the medium having stored thereon instructions to:

send, to a server, a purchase request for a data file, the purchase request including a peer identifier;

receive, from the server, an address of a second peer having the data file and a first encryption dataset for decrypting the data file;

send, to the second peer, a download request for the data file;

receive, from the second peer, the data file;

decrypt the data file with the first encryption dataset; and

output the data file.

60. (Original) The machine-readable medium of claim 59, wherein the data file is a music file.

61. (Original) The machine-readable medium of claim 59, further comprising instructions to:

receive, from the server, an address of a peer having an advertisement;

download, from the peer having the advertisement, the advertisement; and

play the advertisement.

62. (Original) The machine-readable medium of claim 59, further comprising an instruction to send a password to the server before receiving the address of a second peer having the data file and the first encryption dataset for decrypting the data file.

63. (Original) The machine-readable medium of claim 59, further comprising an instruction to send, to the server, a confirmation signal confirming receipt of the data file.

64. (Original) The machine-readable medium of claim 59, further comprising an instruction to send, to the server, a signal indicating inability to download the data file when unable to download the data file.

65. (Original) The machine-readable medium of claim 64, further comprising an instruction to receive an address of a third peer having the data file after sending the signal indicating inability to download the data file.

66. (Original) The machine-readable medium of claim 59, wherein the first encryption dataset includes an encrypted private transaction key.

67. (Original) The machine-readable medium of claim 66, wherein the encrypted private transaction key is decipherable only by the first peer.

68. (Original) The machine-readable medium of claim 66, wherein the instruction to decrypt the data file further uses a private key known only to the first peer.

69. (Original) The machine-readable medium of claim 59, further comprising:

storing an encrypted copy of the data file; and

notifying the server that the data file is stored.

70. (Original) A peer in a peer-to-peer system, comprising:

a peer identification; and

an engine capable to

send, to a server, a purchase request for a data file, the purchase request including a peer identifier;

receive, from the server, an address of a second peer having the data file and a first encryption dataset for decrypting the data file;

send, to the second peer, a download request for the data file;

receive, from the second peer, the data file;

decrypt the data file with the first encryption dataset; and

output the data file.

71. (Original) The peer of claim 70, wherein the data file is a music file.

72. (Original) The peer of claim 70, wherein the engine is further capable to:

receive, from the server, an address of a peer having an advertisement;

download, from the peer having the advertisement, the advertisement; and

play the advertisement.

73. (Original) The peer of claim 70, wherein the engine is further capable to send a password to the server before receiving the address of a second peer having the data file and the first encryption dataset for decrypting the data file.

74. (Original) The peer of claim 70, wherein the engine is further capable to send, to the server, a confirmation signal confirming receipt of the data file.

75. (Original) The peer of claim 70, wherein the engine is further capable to send, to the server, a signal indicating inability to download the data file when unable to download the data file.

76. (Original) The peer of claim 75, wherein the engine is further capable to receive an address of a third peer having the data file after sending the signal indicating inability to download the data file.

77. (Original) The peer of claim 70, wherein the first encryption dataset includes an encrypted private transaction key.

78. (Original) The peer of claim 77, wherein the encrypted private transaction key is decipherable only by the first peer.

79. (Original) The peer of claim 77, wherein the engine is further capable to decrypt the data file using the private transaction key and a private key known only to the first peer.

80. (Original) The peer of claim 70, further comprising:

storing an encrypted copy of the data file; and

notifying the server that the data file is stored.

81. (Original) A peer for use in a peer-to-peer system, the peer comprising:

means for sending, to a server, a purchase request for a data file, the purchase request including a peer identifier;

means for receiving, from the server, an address of a second peer having the data file and a first encryption dataset for decrypting the data file;

means for sending, to the second peer, a download request for the data file;

means for receiving, from the second peer, the data file;

means for decrypting the data file with the first encryption dataset; and

means for outputting the data file.

(9) Evidence Appendix

No evidence under 37 C.F.R. §1.130 – 1.132 has been submitted.

(10) Related Proceedings Appendix

There are no decisions rendered by a court or the Board in any proceedings identified pursuant to paragraph (c)(1)(ii) of §41.37.

Respectfully submitted,
Brian Yen

Date: 6/7/06

By _____
Aaron Wininger
Attorney for Applicant
Reg. No. 45,229

Squire, Sanders & Dempsey L.L.P.
600 Hansen Way
Palo Alto, CA 94304-1043
Telephone (650) 856-6500
Facsimile (650) 843-8777